REMARKS / ARGUMENTS

In response to the Office Action mailed February 26, 2007, the Examiner's objection and rejections have been considered. Claims 1, 30, 35, 41, 43, and 48 have been amended. Applicants respectfully traverse the objection and rejections, and earnestly solicit allowance of these claims.

1. Claim Objection – 35 U.S.C. § 132(a) – Amendment filed December 6, 2006

The Examiner objected to the amendment filed on December 6, 2006, based on 35 U.S.C. § 132(a) as introducing new matter. With regard to all pending claims 1, 2, 4-8, 10-41, 43-49, and 51-76,

> [t]he Examiner has reviewed the specification and [is] unable to locate support for the amendments submitted. Moreover, the Examiner has reviewed the remarks and Applicant has not indicated by page and line number where such support exists. Therefore, Applicant should provide where in the specification, by page and line number, support exists for each of the amendments to the claims.

(Office Action, p. 2, ll. 10-14, emphasis added). The objection is respectfully traversed.

The limitation, "the authenticator including a challenge and response system for authenticating the location of the user" (emphasis added) is supported by the Specification in at least the following five locations:

- The system, in accordance with the present invention, may also include a system for determining the identity of the user, which may comprise a challenge and response system, wherein the authenticating server may issue a security challenge to the client, and the client may interrogate the security challenge, generate a response, and send the response to the authenticating server. (p. 4, ll. 18-22, emphasis added).
- The authenticating server 20 in the system 10 may further include a database of authorized locations, for enabling verification of the location of the user as an authorized location. It may further include a system for determining the identity of the user, which may comprise a challenge and response system, such as, for example, software providing challenge/response authentication, or software supporting a public key infrastructure. In the challenge and response system, the authenticating server 20 may issue a security challenge to the user request enabling device 16 to verify the identity of the user. The security challenge may be issued by the authenticating server 20 in the form of a token. The client 16 may then interrogate the security challenge, generate a response, and transmit the response to the authenticating server 20. In such a

system, the authenticating server 20 may include a database for enabling verification of the response of the client 16 to the security challenge, and for enabling authorization of access to the application server 14. (p. 10, ll. 4-17, emphasis added).

- The client 16 connects to the ISP 46 through the Web server 52. The access server 18 captures relevant information regarding the geographic location of the client 16, which information may comprise ANI and DNIS. These values are interpreted by the RADIUS server 20. The RADIUS server 20 validates the user, and issues a challenge including a security token to the client 16. The client 16 interrogates the security token and receives a response which is then transmitted to the ISP 46. The RADIUS server 20 verifies the response based on values in a user accounts database 54. Upon successful verification, the RADIUS server 20 authorizes access to the ISP Web server 52 from the access server 18. (p. 14, ll. 11-20, emphasis added).
- The RADIUS server 20 generates a challenge including a security token to the client 16, which is transmitted by the Web server 52 through the Web proxy server 56 and the ISP 46. The client 16 receives the challenge and queries the security token for a response. The client 16 then transmits the response to the ISP 46. The ISP 46 then transmits the response to the Web proxy server 56, which may again resolve any mapping changes of the IP address and port number 48 to the original session identification of the user name and session identifier 58. The response message is then transmitted to the Web sever 52. The Web server 52 sends the response to the RADIUS server 20 for verification of authenticity. (p. 15, ll. 11-20, emphasis added).
- Upon verification of the user's jurisdictional location by the RADIUS server, the user is prompted to insert the gaming card into the card reader. At this point, if ANI is missing from the data string, the call will be rejected. Upon insertion of the Smart Card, a challenge is issued from the RADIUS server to the client; At this stage, the user inputs a personal identification number which is used to create a response to the server's challenge; Upon validation of the challenge, the gaming system allows access to a desired URL through the client browser. (p. 17, ll. 8-16, emphasis added).

The limitation, "wherein the first number authenticating system relies on user input and does not rely on GPS" (emphasis added) is supported by the Specification in at least the following two locations:

- The RADIUS server can include a system for authenticating the dialer number, which may be accomplished via Automatic Number Identification (ANI) system, and a system for identifying the first number from which the user has dialed, which may be accomplished via a Dialed Number Identification Services (DNIS) system. (p. 4, ll. 11-15, emphasis added).

- Further, in such a dialing system, the authenticating server 20 may include a system for identifying the first number from which the user has dialed, to prevent a user from attempting to circumvent the system 10, *e.g.*, by activating the dialer at the user location 12 from a location other than the user location 12, Such a first number identifying system may comprise, by way of example only, Dialed Number Identification Services (DNIS). (p. 9, l. 28 - p. 10, 1. 3 emphasis added).

In view of the support identified above, it is respectfully requested that the objection be withdrawn.

2. Claim Rejections – 35 U.S.C. § 103(a) – Claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76

The Examiner rejected claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76 under 35 U.S.C. § 103(a) as being obvious over Goertzel in view of Shaffer.

Independent claims 1, 30, 35, 41, 43, and 48 include the feature, "the authenticator including a challenge and response system for authenticating the location of the user." (emphasis added). The Examiner asserted that Goertzel's location detection mechanism 71 of FIG. 4 discloses this feature. However, the location discrimination mechanism 71 simply "assign[s] IP addresses in one range for callers from 'authorized' phone number[s]." (Goertzel, 6:35-39). Contrary to the Examiner's opinion, Goertzel's location discrimination mechanism 71 is not related to and does not provide any "challenge and response."

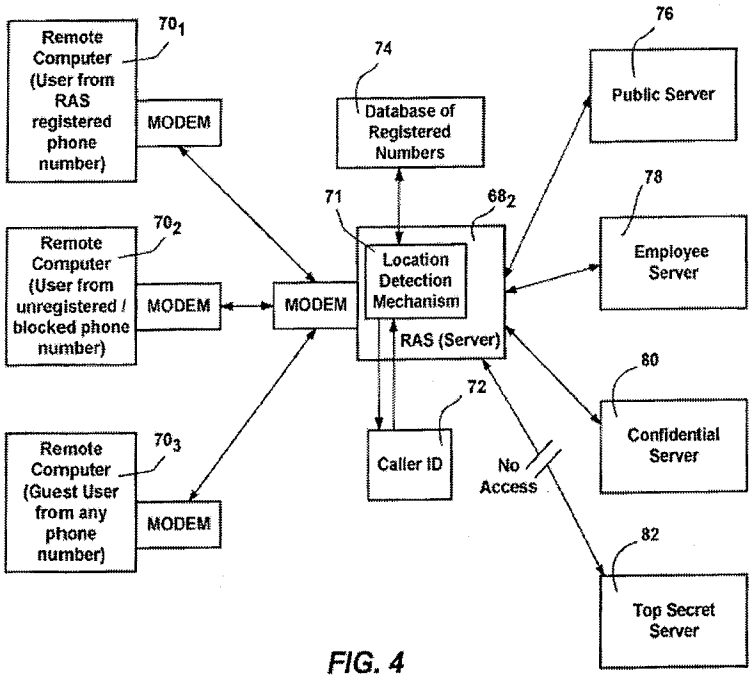

FIG. 4

Additionally, claims 1, 30, 35, 41, 43, and 48 include the feature, "the first number authenticating system relies on user input and does not rely on GPS." The Examiner asserted that

> Shaffer . . . teaches a communication system and method wherein the location of a remote user is determined (columns 16-17). Furthermore, Shaffer utilizes ANI, DNIS and geographic identifier in order to determine the identity and location of the caller (see also columns 25-29).

(Office Action, p. 4, ll. 1-4). Shaffer is directed to a Voice Response Unit (VRU), also known as Interactive Voice Response (IVR), for use in a call processing center (Shaffer, 1:59-65).

> The VRU receives network provided data, such as automatic number identification (ANI) and dialed number identification service (DNIS), and caller-provided data, such as data entered by Dual Tone Multi-Frequency (DTMF) through a Touchtone telephone key pad or the caller speaking through the telephone to a VRU. (Shaffer, 2:19-25).
>
> The VRU validates that the received telephone number is a valid ten digit phone number. (Shaffer, 16:1-12).

With precision, Shaffer discloses that the caller's identity and geographic location are determined by relating an automatic number identification (ANI) or a caller-id of the caller with "databases for spatial, geographic, USPS address, household, individual, business location, government location, business financial, property and client service locations." (Shaffer, 4:38-59). Shaffer's determination of an USPS address based on an ANI or a caller-id of a telephone call is not relevant to first number authentication.

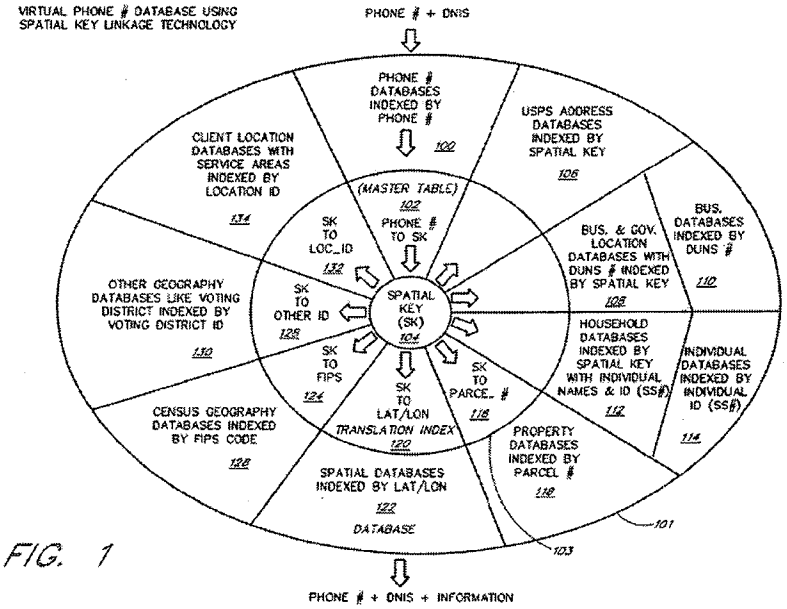

FIG. 1

Shaffer falls short in determining both (a) the identity of the user and (b) whether the user is in a particular geographic location (*i.e.*, Las Vegas) when a computer in Las Vegas attempts to access a casino's computer in a particular geographic location (*i.e.*, Reno). Shaffer cannot

prevent a user in another geographic location (*i.e.*, Alexandria) from controlling the computer in Las Vegas via a computer in Alexandria, and causing the computer in Las Vegas to connect to the casino's computer in Reno. Although Shaffer may identify the USPS address associated with the Las Vegas computer calling the Reno casino's computer, Shaffer fails to identify or locate the originating user. Therefore, Shaffer does not disclose, teach, or suggest the claimed "first number authentication." (emphasis added).

In sum, independent claims 1, 30, 35, 41, 43, and 48 are patentable over Goertzel in view of Shaffer because neither Goertzel nor Shaffer disclose, teach, or suggest the claimed limitations, "the authenticator including a challenge and response system for authenticating the location of the user" and "wherein the first number authenticating system relies on user input and does not rely on GPS." (emphasis added).

Claims 2, 4-8, 10-21, 23, 24, and 26-29 are patentable over Goertzel in view of Shaffer at least by virtue of their dependence from claim 1. Claims 31-34 are patentable over Goertzel in view of Shaffer at least by virtue of their dependence from claim 30. Claims 36-40 are patentable over Goertzel in view of Shaffer at least by virtue of their dependence from claim 35. Claims 44-47 are patentable over Goertzel in view of Shaffer at least by virtue of their dependence from claim 43. Claims 49, 51-68, and 70-76 are patentable over Goertzel in view of Shaffer at least by virtue of their dependence from claim 48.

3. Claim Rejections – 35 U.S.C. § 103(a) – Claims 22, 25 and 69

The Examiner rejected claims 22, 25, and 69 under 35 U.S.C. § 103(a) as being obvious over Goertzel in view of Shaffer, and further in view of Paravia.

Nothing in Paravia discloses, teaches, or suggests the deficiencies of Goertzel and Shaffer. Therefore, claims 22, 25, and 69 are patentable over Goertzel in view of Shaffer, and further in view of Paravia at least by virtue of their respective dependence from claims 1 and 48.

CONCLUSION

Applicants have made an earnest and *bona fide* effort to clarify the issues before the Examiner and to place this case in condition for allowance. Reconsideration and allowance of all of claims 1, 2, 4-8, 10-41, 43-49, and 51-84 is believed to be in order, and a timely Notice of Allowance to this effect is respectfully requested.

The Commissioner is hereby authorized to charge the fees indicated in the Fee Transmittal, any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17, or to credit any overpayments, to Deposit Account No. 194293, Deposit Account Name STEPTOE & JOHNSON LLP.

Should the Examiner have any questions concerning the foregoing, the Examiner is invited to telephone the undersigned attorney at (310) 734-3200. The undersigned attorney can normally be reached Monday through Friday from about 9:00 AM to 6:00 PM Pacific Time.

Respectfully submitted,

Date: May 29, 2007

Joel G. Landau
Reg. No. 54,732
STEPTOE & JOHNSON LLP
2121 Avenue of the Stars
Suite 900
Los Angeles, CA 90067
Tel 310.734.3200
Fax 310.734.3300